

ABSTRACT OF THE DISCLOSURE

5 A method and apparatus for performing ephemeral
communication and assuring that an ephemeral decryption
key is not accessible subsequent to an expiration time
associated with the respective key. An ephemeral key
pair is preferably generated within a tamper resistant
cryptographic processor unit. The ephemeral key pair
comprises an ephemeral encryption key and an ephemeral
10 decryption key. The ephemeral decryption key is
prevented from being accessed external of the tamper
resistant cryptographic processor unit. Ephemeral
messages encrypted using an ephemeral encryption key are
decrypted by the cryptographic processor unit if
15 associated with a time that precedes the expiration time
for the respective ephemeral decryption key. A decrypted
ephemeral message is prevented from being transmitted
from the cryptographic processor unit in the event a time
associated with a received encrypted ephemeral message is
20 subsequent to the expiration time for the respective
ephemeral key pair.

241084